a cura di: **Andrea Dell'Amico - betaxp86 - 26-10-2011 20:00**

KeySecurePC Platinum

LINK (https://www.nexthardware.com/recensioni/sistemi-operativi/603/keysecurepc-platinum.htm)

Un sistema completo a prova di ladro su USB 3.0.

La sicurezza informatica è uno degli aspetti che più dovrebbe essere curato in ambito aziendale, ma che non sempre è seguito da personale esperto o con adeguate misure tecnologiche.

Negli ultimi anni sono balzati agli onori della cronaca molti casi di furti di notebook o personal computer contenenti miglia di dati sensibili, ponendo dubbi sulla corretta gestione di queste informazioni.

Nella maggior parte dei casi la perdita di un notebook non avviene per dolo, ma per semplice negligenza; ogni giorno vengono infatti ritrovati in aeroporti, stazioni e taxi numerosi dispositivi elettronici che, dopo qualche mese, vengono messi allâ€™asta e che possono essere riacquistati con il loro prezioso contenuto con un valore, in alcuni casi, enormemente superiore rispetto a quello del prodotto stesso.

Molte sono le tecnologie atte a impedire lâ€™accesso non autorizzato ai propri dati personali, ma il loro utilizzo può risultare talvolta complesso e particolarmente macchinoso.

Questâ€™ultimo aspetto è quello che porta lâ€™utente a non utilizzare sistemi crittografici evoluti o password complesse, rendendo le informazioni accessibili virtualmente a chiunque.

KeySecurePC Platinum è un prodotto che viene incontro alle esigenze di protezione della riservatezza dei dati, fornendo un completo ambiente di lavoro criptato avviabile da un drive USB 3.0.

Le tecnologie alla base di KeySecurePC sono open source, tuttavia tutto il software incluso nel prodotto è stato certificato e verificato dal produttore in modo che sia allineato con i requisiti di sicurezza richiesti.

Nel corso di questa recensione analizzeremo i punti di forza e le debolezze di questo particolare flash drive USB sviluppato dallâ€™omonima azienda italiana.

Buona lettura!

↔

1. KeySecurePC

1. KeySecurePC

↔

Lâ€™aspetto esteriore di KeySecurePC è quello di una penna USB 3.0 di elevata capacità , motivo per cui le dimensioni sono decisamente maggiori rispetto alle tradizionali Pen Drive USB 2.0.

Dato lâ€™ingombro della penna, infatti, non è possibile utilizzare le porte USB adiacenti a quella in

uso dal dispositivo.

↔

↔

↔

KeySecurePC S.p.A. ha deciso di utilizzare un dispositivo ad alte prestazioni con velocità in lettura↔ e scrittura rispettivamente pari a 204MB/s e 96MB/s, dotato quindi di un controller piuttosto evoluto e memorie NAND di qualità .

Il controller è affiancato da 64MB di memoria cache ed è equipaggiato con il supporto per la tecnologia Trim e Garbage Collection, in modo da mantenere costanti nel tempo le prestazioni del dispositivo.

KeySecurePC è disponibili in versioni da 16 a 256GB: il drive oggetto della nostra prova è il modello da 64GB.

La compatibilità è garantita con la maggior parte dei computer in commercio dotati di porte USB 3.0 o USB 2.0; potrebbe essere tuttavia necessaria lâ€™installazione di un boot loader dedicato (Bootmanager KeySecurePC), nel caso il produttore della scheda madre non abbia implementato correttamente il boot da periferiche USB ad alte prestazioni.

↔

↔

↔

Lâ€™ambiente di lavoro di KeySecurePC è una distribuzione Linux personalizzata, basata sulla diffusissima Ubuntu, ma dotata di una interfaccia grafica semplificata che ricorda il paradigma del desktop di Microsoft Windows.

Allâ€™interno della memoria del KeySecurePC troviamo sia il sistema operativo che gli applicativi ed i dati dellâ€™utente, il tutto in ambiente crittografato e non accessibile se non utilizzando la password creata durante la fase di setup.

Nessun dato viene memorizzato sui dischi della macchina in uso; di conseguenza, una volta spento il PC e rimosso il KeySecurePC non vi è traccia del proprio lavoro e tutti i dati sono conservati nel dispositivo.

Le applicazioni disponibili per il KeySecurePC sono tutte quelle compatibili con Linux e possono essere scaricate dal Software Center, un comodo gestore di pacchetti personalizzato da KeySecurePC.

Gli aggiornamenti degli applicativi e del sistema operativo possono invece essere eseguiti dallâ€™utility Gestore Aggiornamenti.

Per gli utenti Microsoft Windows è stato integrato il software di emulazione CrossOver Professional che consente lâ€™utilizzo allâ€™interno di Linux di oltre 1400 applicativi Windows, senza la necessità di utilizzare una macchina virtuale completa.

Tra i software supportati troviamo anche la suite di produttività Microsoft Office 2007 e le sue versioni precedenti.

Come tutti i software di emulazione dobbiamo però ricordare che non tutte le funzionalità possono essere disponibili e che la stabilità del prodotto potrebbe non essere paragonabile a quella di una installazione tradizionale.

In abbinamento al KeySecurePC↔ è possibile acquistare unâ€™unità gemella per effettuare il solo Backup Crittografato dellâ€™unità principale, funzionalità accessibile allâ€™interno del prodotto.

In alternativa allâ€™unità di Backup fornita da KeySecurePC, è possibile utilizzare un disco fisso o una penna USB tradizionale, ma si dovrà provvedere manualmente alla crittografia dei dati con prodotti di terze parti.

↔

2. Crittografia AES 256 e Partizioni

2. Crittografia AES 256 e Partizioni

↔

AES 256

Lâ€™algoritmo alla base della sicurezza del KeySecurePC è lâ€™AES256 (Advanced Encryption Standard), uno dei più diffusi algoritmi crittografici con cifratura a blocchi, utilizzato come standard dal governo degli Stati Uniti dâ€™America.

AES256 è un algoritmo a chiave simmetrica dalle elevate prestazioni, di semplice implementazione e la cui sicurezza è ad oggi ancora inviolata, anche se sono stati eseguiti molti tentativi di "forzatura" nellâ€™ultimo decennio.

La lunghezza della chiave è, come si può intuire dal nome, di 256bit, più che sufficiente per ovviare ad un possibile attacco di forza bruta sulla stessa, che richiederebbe, con le attuali tecnologie, decenni di computazione.

A titolo di confronto, lâ€™impostazione di default per la crittografia del disco BitLocker di Microsoft Windows 7 è lâ€™AES128 (chiave a 128bit), estendibile a 256bit per aumentare la sicurezza del sistema.

Per maggiori informazioni riguardo allâ€™algoritmo AES, vi rimandiamo alla pagina dedicata su Wikipedia (http://it.wikipedia.org/wiki/Advanced_Encryption_Standard).

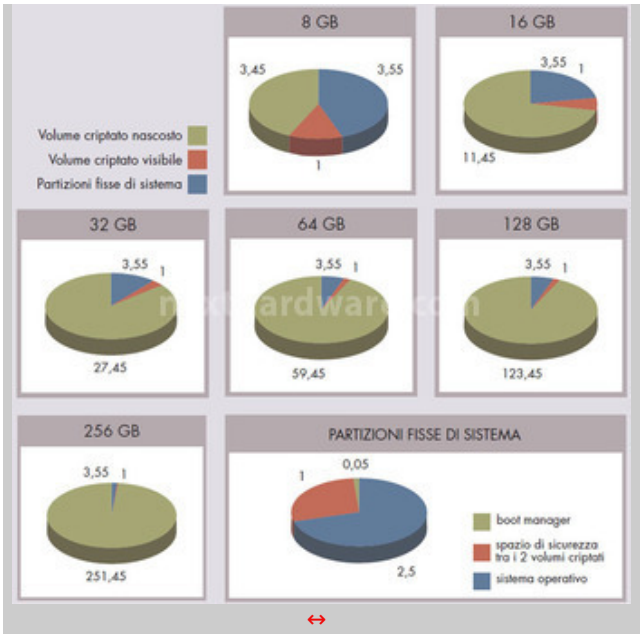
↔

Partizioni

Sono previsti due ambienti di lavoro nel KeySecurePC, il primo risiede in una partizione criptata da 1GB ed è visibile alla maggior parte dei tool di gestione dei dischi, il secondo, che occupa gran parte dello spazio disponibile, è anchâ€™esso criptato ma risulta completamente invisibile e non accessibile al di fuori del controllo del dispositivo.

Una terza partizione, hidden FAT32 senza crittografia, contiene i file di boot del sistema (kernel, ramdisk, boot loader) ed una immagine compressa dello stesso. ↔

↔



Partizioni KeySecurePC

Lo spazio effettivamente utilizzabile varia in funzione della capacità del Pen Drive; come acennato, nel primo ambiente di lavoro solo 1GB di partizione criptata è visibile all'utente.

Durante la fase di boot, lâ€™immagine compressa viene montata in sola lettura e viene unita al volume criptato dove risiedono, oltre ai dati dellâ€™utente, anche eventuali aggiornamenti del sistema operativo, nuovi software installati e le configurazioni personalizzate.

In questo modo è possibile ripristinare le condizioni originali del KeySecurePC senza occupare ulteriore spazio per una immagine di BackUp del sistema originale che viene mantenuto integro e aggiornato solo nei componenti necessari nella partizione criptata.

↔

3. Distruzione volontaria dei dati (Wiping)

3. Distruzione volontaria dei dati (Wiping)

↔

La distruzione volontaria dei dati è una procedura che consente la totale cancellazione di tutte le informazioni presenti su un supporto di memorizzazione ed è prevista dalla legislazione di molti paesi prima delle dismissione di un sistema informativo, soprattutto in ambito governativo.

Le procedure di cancellazione dei dati sono differenti in base al dispositivo utilizzato e possono richiedere da pochi secondi a diverse ore per essere effettuate.

I procedimenti più rapidi per la cancellazione di un Hard Disk tradizionale sono quelli meccanici, che grazie allâ€™utilizzo di particolari presse o generatori di forti campi magnetici distruggono fisicamente il dispositivo.

Queste apparecchiature risultano però piuttosto costose e a solo appannaggio di grandi aziende e istituzioni, per cui si tende a ricorrere a software che sovrascrivono un numero sufficiente di volte ogni settore per garantire la cancellazione dei dati.

Questa operazione richiede ovviamente molte ore per essere completata e spesso non viene effettuata, confidando, erroneamente, che nessuno andrà a â€œsbirciareâ€ nei nostri Hard Disk dopo la loro dismissione o vendita.

↔

Con l'inserimento della password di Wiping vengono distrutti tutti i dati contenuti nei KeySecurePC in meno di 3 minuti.

↔

KeySecurePC integra un sistema di Wiping per la distruzione di tutti i suoi contenuti e del sistema operativo stesso.

La funzionalità può essere richiamata sia dalla schermata di login, inserendo unâ€™apposita password scelta durante lâ€™inizializzazione del dispositivo, sia dallâ€™icona presente sul desktop o nel menù Start.

Il processo dura solo pochi minuti e prevede la distruzione di tutte le partizioni presenti sul disco e degli identificatori delle stesse, rendendo il KeySecurePC un semplice Pen Drive USB 3.0.

Non è possibile ripristinare in modo autonomo le funzionalità del dispositivo dopo averne effettuato il Wiping; è necessario quindi contattare lâ€™azienda produttrice per reinizializzare il dispositivo.

Nel caso si desiderasse semplicemente ripristinare il prodotto nelle condizioni originali, non va effettuato il Wiping ma la procedura di Inizializzazione del Dispositivo presente nel menù KeySecurePC.

↔

↔

4. Inizializzazione, Aggiornamenti e Driver

4. Inizializzazione, Aggiornamenti e Driver

↔

Al primo avvio del KeySecurePC è necessario impostare tre password di sicurezza:

- Dedicata allâ€™accesso Ospite al sistema, con una ridotta disponibilità di spazio disco.
- Dedicata allâ€™acceso Completo al sistema, può disporre dellâ€™intera capacità del Pen Drive.
- Dedicata al Wiping del dispositivo, consentendo la distruzione di tutti i dati.

↔

↔

Secondo le specifiche del produttore questa operazione può richiedere dai 3 ai 70 minuti, nelle nostre prove su un Notebook Sony serie SB, utilizzando la porta USB 3.0, lâ€™intero processo non

ha richiesto più di 5 minuti.

Una volta avviato il sistema potremo procedere agli aggiornamenti del software installato utilizzando lâ€™applicativo â€œGestore aggiornamentiâ€ disponibile al percorso Start -> Sistema -> Amministrazione.

La verifica della presenza di nuovi aggiornamenti viene effettuata ogni giorno e lâ€™utente può decidere se debbano essere installati automaticamente o se debbano essere solo notificati.

↔

I software aggiuntivi possono essere installati dal Software Center con un semplice click sul prodotto desiderato.

Di default solo le repository di software del KeySecurePC sono abilitate al download, limitando il numero di programmi disponibili e gli aggiornamenti degli stessi.

A nostro avviso è consigliabile modificare questa impostazione, selezionando anche le altre sorgenti.

Per gli utenti Linux più esperti è ovviamente possibile installare software seguendo le tradizionali procedure manuali o con il gestore Apt-Get.

Nel caso il nostro Hardware necessitasse dellâ€™installazione di driver proprietari, possiamo procedere allâ€™attivazione degli stessi dal pannello â€œDriver hardwareâ€.

Come policy standard di molte distribuzioni Linux i driver non Open Source non vengono attivati di default, ma sono necessari per il corretto utilizzo dei più recenti modelli di schede video o altre periferiche non standard.

↔

5. CrossOver Professional - Virtual Box

5. CrossOver Professional - Virtual Box

↔

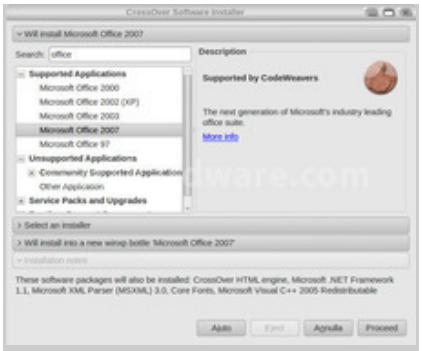
CodeWeavers ↔ CrossOver Professional

CrossOver Professional è un software di emulazione di Windows per i sistemi operativi Linux e Mac prodotto da CodeWeavers, la cui prima versione fu rilasciata nel 2002 consentendo agli utenti Linux di eseguire Microsoft Office e Internet Explorer sullâ€™ancora giovane sistema operativo del â€œpinguinoâ€.

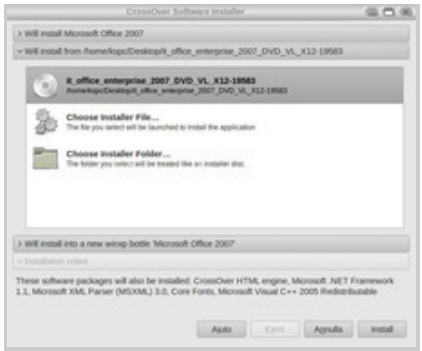
CrossOver utilizza un layer di emulazione che simula le API di Windows ingannando il software in esecuzione e confinandolo in una â€œBottlesâ€, una sorta di contenitore che ingloba tutte le componenti del programma e dei suoi prerequisiti, simulando, inoltre, il file System di Windows.

Possono essere presenti più â€œBottlesâ€ nello stesso sistema, garantendo la completa separazione tra i vari applicativi installati allâ€™interno di CrossOver per evitare eventuali problemi di incompatibilità .

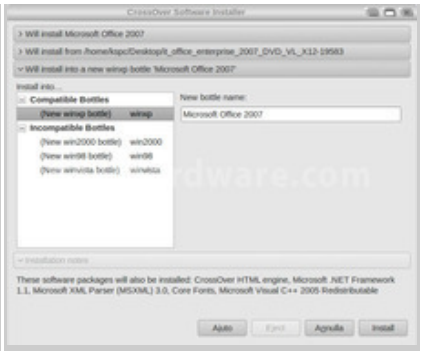
↔



Applicativo da installare



Sorgente installazione



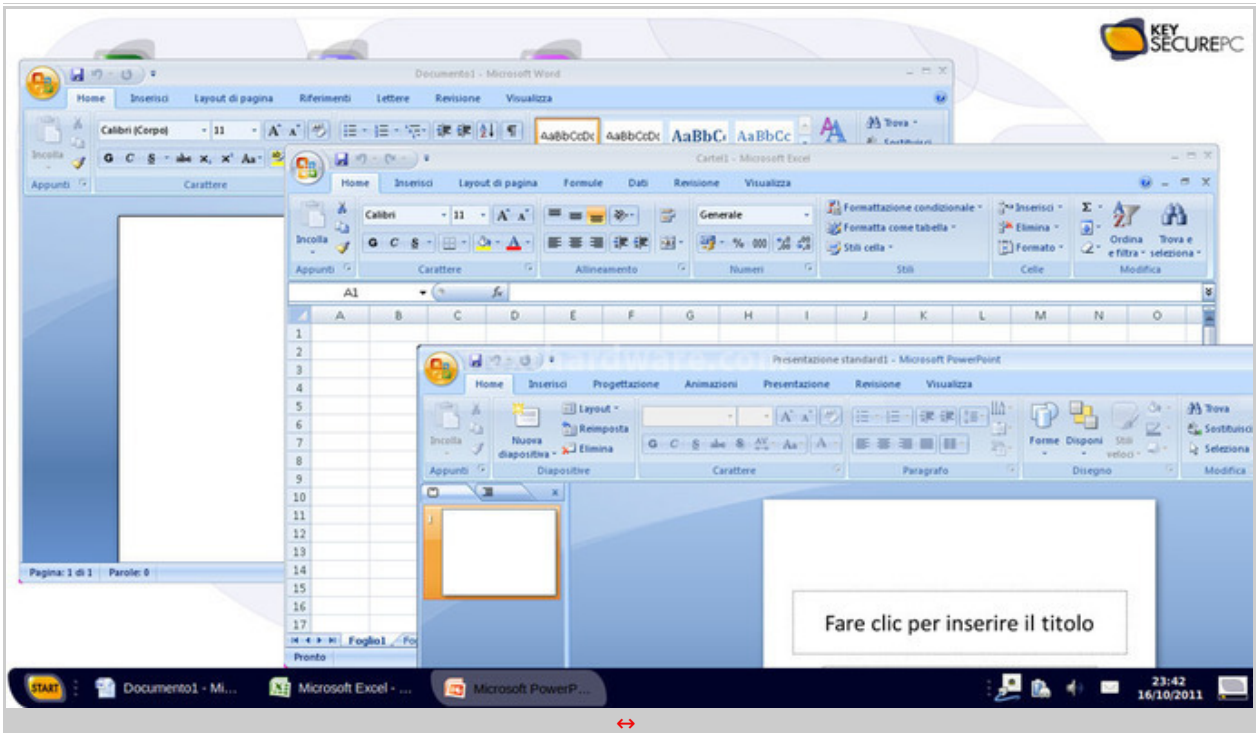
Creazione della Bottle

Installare un software allâ€™interno di CrossOver Professional è piuttosto semplice e richiede solo pochi minuti seguendo la procedura guidata.

Nel caso di installazione di software complessi, potrebbe essere necessario installare alcuni requisiti che saranno automaticamente caricati nel sistema allâ€™avvio dellâ€™installazione.

Per le nostre prove abbiamo installato Microsoft Office 2007 Enterprise, completando il processo in pochi minuti e senza particolari problemi.

↔



KeySecurePC con CrossOver e Microsoft Office 2007

Gli applicativi risultano integrati con le funzionalità di copia e incolla del sistema operativo e possono accedere alle risorse dei dischi locali.

Durante lâ€™esecuzione abbiamo assistito ad alcuni crash, ma per stessa ammissione di CodeWeavers non è possibile garantire la completa compatibilità dei vari programmi in esecuzione su una piattaforma completamente diversa.

Attualmente sono 1400 i software che, a vari livelli, CodeWeavers dichiara compatibili (http://www.codeweavers.com/compatibility/browse/name/) con il suo software e la lista è in continuo aggiornamento.

KeySecurePC include la versione Professional di CrossOver garantendo la massima flessibilità nellâ€™uso di questo applicativo.

↔

Oracle VM Virtual Box

Se lâ€™applicativo di cui abbiamo bisogno non è supportato da CrossOver Professional, possiamo affidarci ad un software di virtualizzazione tradizionale.

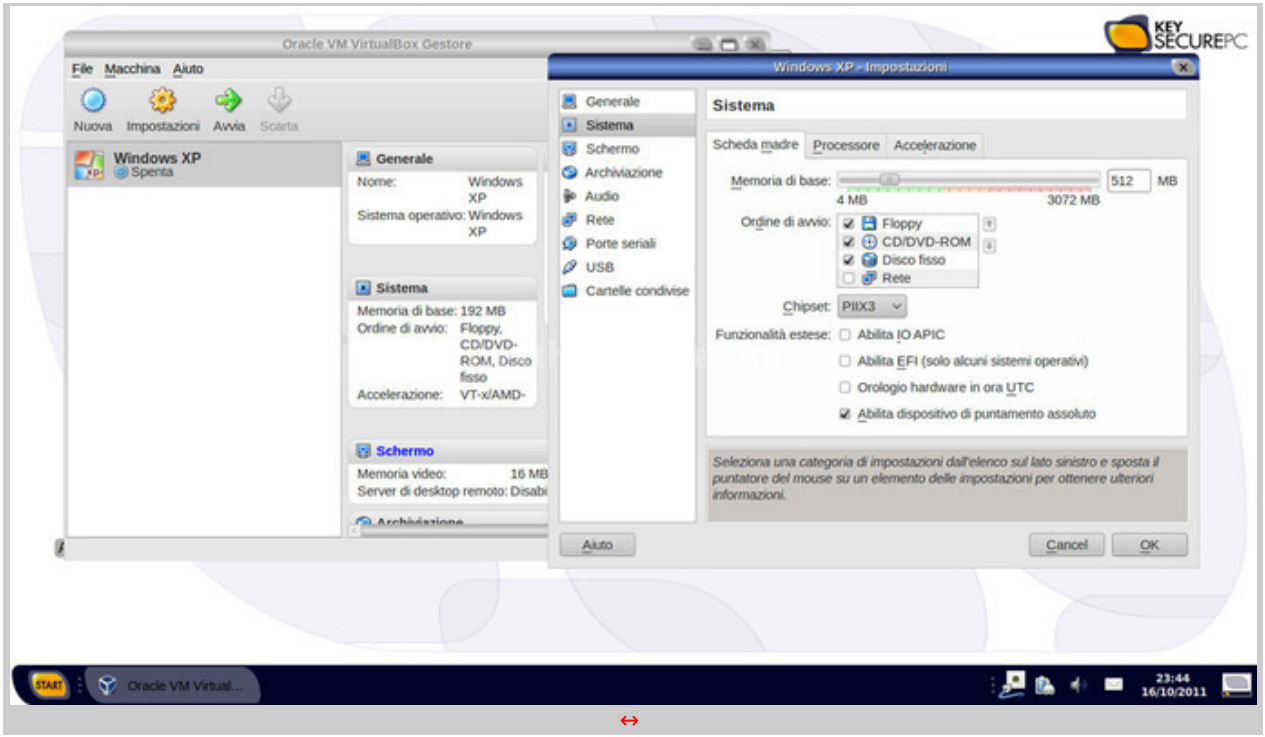
Una delle migliori soluzioni per i sistemi Linux è indubbiamente Oracle VM Virtual Box.

Virtual Box supporta praticamente tutti i sistemi operativi da BSD ai più recenti prodotti di Microsoft, supportando le estensioni VT dei moderni processori AMD e Intel e un primitivo supporto alla grafica 3D.

Oracle VM Virtual Box non è disponibile dal Software Center, ma può essere tuttavia scaricato in formato .deb dal sito del produttore.

La versione da utilizzare è quella destinata alle macchine Ubuntu 10.4 da cui KeySecurePC deriva; lâ€™installazione sarà completamente automaticamente senza richiedere ulteriori interventi da parte dellâ€™utente.

↔



↔

KeySecurePC con Oracle VM Virtual Box e Microsoft Windows XP

Nella creazione di una nuova macchina virtuale possiamo decidere quante risorse allocare a questâ€™ultima variando il numero di processori virtuali, la quantità della memoria RAM o la dimensione del disco fisso.

Per i soli sistemi Microsoft Windows è possibile integrare le finestre degli applicativi in esecuzione dentro la macchina virtuale allâ€™interno del desktop di KeySecurePC, rendendo lâ€™esperienza dâ€™uso ottimale anche per gli utenti meno esperti o che si affacciano per la prima volta al mondo della virtualizzazione.

↔

6. Esperienza d'uso

6. Esperienza dâ€™uso

↔

Lâ€™indubbio vantaggio nellâ€™utilizzo di KeySecurePC rispetto ad un sistema operativo tradizionale, è la possibilità di migrare il proprio ambiente di lavoro da una macchina allâ€™altra senza la necessità di alcuna configurazione, se non il cambio delle sequenza di boot per avviare il pc dal KeySecurePC.

Abbiamo testato KeySecurePC su differenti macchine a partire da un Netbook di prima generazione su USB 2.0, per finire su una piattaforma Intel Z68 Express collegandolo alle porte USB 3.0.

Praticamente tutto lâ€™hardware è stato sempre riconosciuto fin dal primo avvio, ad eccezione dei driver della scheda video AMD utilizzata nella prova sul desktop, che ha richiesto lâ€™attivazione dei driver proprietari dallâ€™apposito pannello di configurazione.

In caso di problemi con specifiche schede audio o di rete è necessario utilizzare i tradizionali strumenti di Linux per risolvere i problemi, operazione non certo alla portata di utente medio.

Con nostro grande stupore, le performance in modalità USB 2.0 sono state piuttosto buone e i tempi di risposta contenuti anche eseguendo una macchina virtuale Microsoft Windows XP in background con un applicativo di produttività al suo interno.

Collegando il KeySecurePC ad una porta USB 3.0 la velocità del sistema è aumentata in modo sensibile, rendendo la copia dei file da rete e dai dischi interni della macchina paragonabile a quella di molti SSD di fascia media.

↔

↔

KeySecurePC con Office 2007 connesso alla rete locale e WiFi

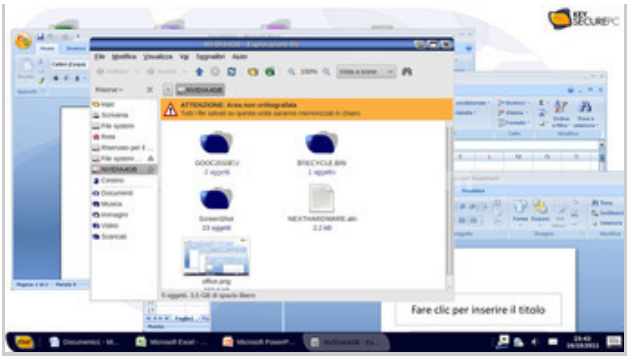
Lâ€™interfaccia grafica è abbastanza comoda da usare ed è familiare anche per chi arriva dai sistemi operativi Microsoft: risulta evidente come le personalizzazioni effettuate da KeySecurePC siano proprio per evitare â€œtraumiâ€ agli utenti.

Dal punto di vista della sicurezza dei dati la crittografia AES256 è completamente trasparente allâ€™utente e non câ€™è un impatto sensibile sulle prestazioni.

Tuttavia, dobbiamo ricordare che non è possibile cambiare la password principale dopo lâ€™inizializzazione e che la sicurezza del sistema è strettamente vincolata alla complessità di questa password, che andrà quindi scelta con molta cura.

↔

Pannello di Controllo



Avviso supporto non sicuro

↔

Tutti i dischi di sistema e penne USB sono accessibili da KeySecurePC, tuttavia su ogni partizione non crittografata è sempre presente un avviso che avverte lâ€™utente dei rischi che incorre a salvare documenti in â€œluoghiâ€ non sicuri.

Il browser predefinito è la versione 3.6 di Firefox, decisamente obsoleta e non aggiornata automaticamente dal â€œGestore aggiornamentiâ€; per ovviare a questo â€œproblemaâ€ è possibile installare manualmente lâ€™ultima versione stabile, aprendo un terminale e digitando i seguenti comandi:

- sudo add-apt-repository ppa:mozillateam/firefox-stable
- sudo apt-get update
- sudo apt-get install firefox

La suite di produttività inclusa è OpenOffice.org 3.2, ma per chi non può fare a meno di Microsoft Office è comunque possibile installarlo attraverso CrossOver come già descritto in precedenza.

↔

7. Conclusioni

7. Conclusioni

↔

KeySecurePC Platinum è un prodotto dedicato allâ€™utenza professionale con specifiche richieste di sicurezza.

I potenziali utenti sono Medici, Avvocati e Notai, tutte categorie professionali che fanno della riservatezza dei dati dei clienti il bene più prezioso.

KeySecurePC risulta un prodotto vincente per chi vuole avere sempre con se il proprio ambiente di lavoro protetto da crittografia avanzata senza dover curarsi dellâ€™hardware sottostante.

I requisiti di KeySecurePC sono tali da consentire il corretto funzionamento del sistema anche su sistemi che oggi sarebbero considerati obsoleti.

Il flash drive USB potrebbe, inoltre, rappresentare lâ€™ideale compagno di un mini PC le cui limitate risorse hardware possono essere comunque sufficienti per lavorare con il sistema Linux integrato.

Se dal punto di vista della sicurezza lâ€™unico potenziale punto debole è la complessità della password dellâ€™utente, sotto il punto di vista dellâ€™usabilità dobbiamo fare alcune doverose considerazioni.

- Lâ€™interfaccia grafica è familiare, ma non tutti sono disposti a cambiare le proprie abitudini per passare ad un sistema operativo differente, basti pensare alle difficoltà di adattamento di molti utenti da Windows XP a Windows 7.
- La compatibilità con le applicazioni Windows è garantita solo attraverso CrossOver o la virtualizzazione di una macchina Windows che richiede la stessa manutenzione di un sistema tradizionale.
- Eventuali modifiche al sistema operativo o installazioni di driver personalizzati e applicazioni devono essere effettuate con gli strumenti tradizionali di Linux, decisamente potenti, ma complessi da utilizzare per un utente medio.

↔

↔

KeySecurePC Platinum

Crittografia AES256

Ambiente portabile su Pen Drive USB 3.0

Funzione di Wiping rapido

Lavorare allâ€™interno del KeySecurePC mette al riparo da eventuali virus, rootkit o keylogger installati nella macchina ospite e consente di operare in totale sicurezza sia online che offline.

Ovviamente un costante aggiornamento del prodotto è necessario per risolvere eventuali falle di sicurezza introdotte dai software in esecuzione.

Il doppio ambiente di lavoro consente una certa flessibilità e la possibilità di condividere il KeySecurePC anche con altri utenti mantenendo intatta lâ€™integrità dei dati e del sistema.

La funzionalità di Wiping è, a nostro avviso, utile solo al termine della vita utile del prodotto, cioè quando il dispositivo sarà da smaltire secondo le vigenti normative di legge sulla protezione dei dati personali.

Nota dolente per la maggior parte degli utenti è il prezzo del KeySecurePC Platinum pari a 650,00 + IVA per il modello da 64GB; costo giustificabile solo in ristretti ambiti lavorativi, per i quali del resto è stato espressamente progettato, e non per uso strettamente personale.

↔

Si ringrazia KeySecurePC S.p.A. (http://www.keysecurepc.com/it/) per averci inviato il sample oggetto di questa recensione.

↔

↔